UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/443,204	11/18/1999	JOHN EDWARD FETKOVICH	EN998146	6903

30400 7590 12/29/2005

HESLIN ROTHENBERG FARLEY & MESITI P.C.
5 COLUMBIA CIRCLE
ALBANY, NY 12203

EXAMINER	
HENEGHAN, MATTHEW E	
ART UNIT	PAPER NUMBER
2134	

DATE MAILED: 12/29/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/443,204	FETKOVICH ET AL.	
	Examiner	Art Unit	
	Matthew Heneghan	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on 15 August 2005.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,2,4,5,7-11,13,14,16,17,19,21-29,31,32 and 34-38* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,2,4,5,7-11,13,14,16,17,19,21-29,31,32 and 34-38* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *18 November 1999* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____.

DETAILED ACTION

1. In response to previous final rejection, Applicant appealed the stated rejections, all of which had been made under 35 U.S.C. 103(a), to the Board of Patent Appeals and Interferences. In a decision mailed 14 June 2005, the BPAI reversed all of the Examiner's stated rejections, but made new rejections *sua sponte* to all of the pending claims under 35 U.S.C. 112, first paragraph.

In accordance with 37 CFR 41.50(b)(1), Applicant has submitted an amendment to the claims and the case has been remanded to the Examiner. In the amendment, claims 1, 14, 27, and 28 have been amended and claims 12 and 18 have been cancelled.

2. Claims 1, 2, 4, 5, 7-11, 13, 14, 16, 17, 19, 21-29, 31, 32, and 34-38 have been examined.

3. Examination of the instant application has been reassigned to Examiner Matthew Heneghan.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1, 2, 5, 7-11, 13, 14, 16, 17, 19, and 22-27 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 5,412,730 issued to Jones (Jones '730) in view of U.S. Patent No. 5,805,700 issued to Nardone et al. (Nardone '700) and in further view of U.S. Patent No. 5,933,501 issued to Leppek (Leppek '501).

<u>Claims 1, 2, 5, 7, 8, 13, 14, 16, 17, 19, 26, and 27:</u>

Regarding Claim 1, Jones '730 teaches corresponding limitations, specifically a method for protecting a stream of data to be transferred between an encryption unit and a decryption unit (column 12, lines 25-27; Jones '730), said method comprising:

- encrypting the stream of data at a said encryption unit for transferring of said encrypted stream of data from said encryption unit to said decryption unit (column 12, lines 38-39; Jones '730);
- dynamically varying said encrypting of said stream of data at said encryption unit over multiple portions of the streams of data by dynamically changing multiple encryption parameters employed for each portion of the stream of data and signaling said change in encryption parameters to said decryption unit, said dynamically varying of said multiple encryption parameters employed for each portion of the stream of data being responsive to occurrence of a predefined condition in said

stream of data (column 12, lines 32-37 and column 12, lines 40-49; Jones '730); and

- decrypting said encrypted data at the decryption unit, said decrypting accounting for said dynamic varying of said encrypting by said encryption unit using said dynamically changed, multiple encryption parameters (column 12, lines 50-51; Jones '730).

The preferred embodiment of Jones '730 discloses an invention in which "means are employed at both the transmitting and receiving stations to monitor the flow of transmitted data and to advance the random number generator each time the transmitted data satisfies a predetermined condition" (column 1, lines 50-54; Jones '730). This advancement causes the change of the cryptographic key used to encrypt and decrypt the data stream, and thus constitutes dynamic variance.

Jones '730 does not teach "dynamically changing multiple encryption parameters."

Nardone '700 teaches dynamically changing encryption parameters as described in paragraphs 9-10 below. However, Nardone '700 does not explicitly teach setting multiple parameters.

Leppek '501 teaches setting multiple parameters as described in paragraphs 9-10 below.

It would have been obvious to a person having ordinary skill in the art to combine Jones '730, Nardone 700, and Leppek '501 on the basis of the description in paragraphs 9-10 below.

Jones '730, Nardone '700, and Leppek '501 in combination teach the dynamic changing of encryption parameters for each portion of a stream of data (column 3, lines 19-25; Jones '730). Jones '730 explicitly teaches measuring the passage of data via a block counter and using a predetermined length as the criteria on when to change the encryption key. The length of bit stream delineated by the block counter constitutes a portion of the bit stream and varying the encryption key constitutes changing at least one encryption parameter. Jones '730, Nardone '700, and Leppek '501 in combination also address the issue of "multiple parameters" as described in paragraphs 9-10 below.

Regarding Claim 2, Jones '730, Nardone '700, and Leppek '501 in combination teach corresponding limitations, specifically all the limitations of Claim 1 described above, plus specifying at least one encryption parameter that comprises "at least one of an encryption key, an encryption granularity, an encryption density scale, an encryption density, an encryption delay, an encryption key update variable, and an encryption key update data trigger" (column 12, lines 32-37 and column 12, lines 40-49; Jones '730). Jones '730 teaches the varying of the encryption key. Since this encryption key, which is varied, is one of the enumerated parameters, this constitutes varying at least one of the parameters enumerated in Claim 2. Furthermore, regarding Claim 2 as amended, Jones '730, Nardone '700, and Leppek '501 in combination address the issue of "multiple parameters" which also covers the issue of, "at least two parameters", as described in paragraphs 9-10 below.

Regarding Claim 5, Jones '730, Nardone '700, and Leppek '501 in combination teach corresponding limitations, specifically all the limitations of Claim 1 described

above, plus specifying that "dynamically varying said encryption parameter based on passage of a predefined number of units of physical data or passage of a predefined number of conceptual units of data" (column 12, lines 35-37 and column 12, lines 48-49; Jones '730). Jones '730 teaches use of a block counter to measure the data stream in order to determine when to vary the cryptographic key used to encrypt and decrypt the data stream (column 3, lines 33-36 and column 3, lines 64-68; Jones '730). Furthermore, regarding Claim 5 as amended, Jones '730, Nardone '700, and Leppek '501 in combination address the issue of "multiple parameters" as described in paragraphs 9-10 below.

Regarding Claim 7, Jones '730, Nardone '700, and Leppek '501 in combination teach corresponding limitations, specifically all the limitations of Claim 1 described above, plus specifying that the "stream of data comprises a stream a compressed data, and wherein said method further comprises decompressing said compressed data after said decrypting of said encrypted data by said decrypting unit" (column 2, line 29; column 8, line 5, and column 8, lines 16-22; Jones '730).

Regarding Claim 8, Jones '730, Nardone '700, and Leppek '501 in combination teach corresponding limitations, specifically all the limitations of Claim 7 described above, plus specifying that, "said stream of compressed data can comprise one of MPEG encoded video data, MPEG encoded audio data, and Dolby AC-3 audio data" (column 3, lines 12-16; Jones '730). In fact, the method of Jones '730 is independent of the format of the data to be transmitted. Furthermore, there are no non-obvious consequences of choosing to carry MPEG or AC-3 data.

Regarding Claim 13, Jones '730 , Nardone '700, and Leppek '501 in combination teach corresponding limitations, specifically all the limitations of Claim 1 described above, plus specifying, "dynamically varying said at least one encryption parameter responsive to passage of a predefined number of data bits in said stream of data or alternatively, responsive to passage of a predefined number of data units in said stream of data wherein said data units comprise at least one of a program, a sequence, a group of pictures, a slice, or a macroblock" (column 3, lines 19-25; Jones '730). Jones '730 explicitly teaches measuring the passage of data via a block counter and using a predetermined length as the criteria on when to change the encryption key. Varying the encryption key constitutes changing at least one encryption parameter. Furthermore, Jones '730 states that, "Advantageously, the block counter may simply count the number of bytes, words or blocks of data being transmitted ..." (column 3, lines 19-22; Jones '730). In the case of MPEG encoding, an implementer who wished to identify such an advantageous block of data would choose MPEG specific data lengths which include items such as a slice or a macroblock as enumerated in Claim 13. Furthermore, regarding Claim 13 as amended, Jones '730, Nardone '700, and Leppek '501 in combination address the issue of "multiple parameters" as described in paragraphs 9-10 below.

Regarding Claim 14, Jones '730, Nardone '700, and Leppek '501 in combination teach all the limitations of the claim using a similar argument as provided for Claim 1 above. Specifically, Jones '730 teaches a system that encrypts (column 12, lines 38-39; Jones '730) and decrypts (column 12, lines 50-51; Jones '730) data while varying

encryption parameters (column 3, lines 19-25 and column 12, lines 32-37 and column 12, lines 40-49; Jones '730). Furthermore, Jones '730, Nardone '700, and Leppek '501 in combination address the issue of "multiple parameters" as well as the issue of "simultaneous dynamic change", as described in paragraphs 9-10 below.

Regarding Claim 16, Jones '730, Nardone '700, and Leppek '501 in combination teach all the limitations of Claim 15 as described above. Furthermore, Jones '730 teaches the disclosed invention applied to digital data (column 3, lines 13-16; Jones '730).

Regarding Claim 17, Jones '730, Nardone '700, and Leppek '501 in combination teach all the limitations of Claim 14 as described above. Furthermore, Jones '730 teaches varying an encryption parameter according to the passage of bits (column 3, lines 16-25; Jones '730) using a similar argument as provided for Claim 5. Furthermore, regarding Claim 17 as amended, Jones '730, Nardone '700, and Leppek '501 in combination address the issue of "multiple parameters" as described in paragraphs 9-10 below.

Regarding Claim 19 Jones '730, Nardone '700, and Leppek '501 in combination teach all the limitations of Claim 14 as described above. Furthermore, Jones '730 teaches varying at least one encryption parameter (column 12, lines 32-37 and column 12, lines 40-49; Jones '730) using a similar argument as provided for Claim 2 above. Furthermore, regarding Claim 19 as amended, Jones '730, Nardone '700, and Leppek '501 in combination address the issue of "multiple parameters" as described in paragraphs 9-10 below.

Regarding Claim 26, Jones '730, Nardone '700, and Leppek '501 in combination teach all the limitations of Claim 14 as described above. Furthermore, Jones '730 teaches the additional limitation of Claim 26, that an encryption parameter be varied for a block of data (column 3, lines 19-25; Jones '730) using a similar argument as provided for Claim 13 above. Furthermore, regarding Claim 26 as amended, Jones '730, Nardone '700, and Leppek '501 in combination address the issue of "multiple parameters" as described in paragraphs 9-10 below.

Regarding Claim 27, Jones '730, Nardone '700, and Leppek '501 in combination teach corresponding limitations, specifically a system for protecting a stream of data to be transferred between a sender and a receiver (column 1, lines 37-42; Jones '730), said system comprising:

- an encryption unit disposed at said sender for encrypting the stream of data prior to transfer to said receiver, said encryption unit being adapted to dynamically vary encrypting of the stream of data over multiple portions of the stream of data by changing multiple encryption parameters employed for each portion of the stream of data based on an occurrence of a predefined condition in said data stream and signaling said change in encryption parameter employed for each portion of the stream of data to said receiver (column 12, lines 38-39; column 12, lines 32-37; and column 12, lines 40-49; Jones '730); and
- a decryption unit disposed at said receiver for decrypting said encrypted data, said decryption unit being adapted to receive said changed

encryption parameter to account for said dynamic varying of said encrypting by said encryption unit using said changed encryption parameter (column 12, lines 50-51; Jones '730).

The preferred embodiment of Jones '730 discloses an invention in which "means are employed at both the transmitting and receiving stations to monitor the flow of transmitted data and to advance the random number generator each time the transmitted data satisfies a predetermined condition" (column 1, lines 50-54; Jones '730). This advancement causes the change of the cryptographic key used to encrypt and decrypt the data stream, and thus constitutes dynamic variance of at least one encryption parameter.

Furthermore, regarding Claim 27 as amended, Jones '730, Nardone '700, and Leppek '501 in combination address the issue of "multiple parameters" and "dynamically changing parameters simultaneously" as described in paragraphs 9-10 below.

Furthermore, Jones '730 teaches encrypting multiple portions of a bit stream (column 3, lines 19-25; Jones '730) using similar argument as provided for Claim 1 above.

<u>Claims 9-11 and 22-25:</u>

Regarding Claim 9, Jones '730 teaches all the limitations of Claim 1 as described above, including the varying of an encryption key. However, Jones '730 does not teach a "plurality of encryption parameters being employed by said encrypting and wherein said changed encryption parameter of said dynamically varying comprises one encryption parameter of said plurality of encryption parameters." Furthermore, Jones

'730 does not teach "initializing a plurality of encryption parameters based on sensitivity of said stream of data."

Leppek '501 teaches the use of multiple encryption algorithms as described above. Leppek '501 also teaches "initializing a plurality of encryption parameters" (column 4, lines 52-66; Leppek '501) but does not use sensitivity of the bit stream as a criterion for initialization.

Nardone '700 teaches the varying of granularity and density encryption, specifically only encrypting a selected portion of a bit stream as described above. Nardone '700 also teaches "sensitivity of said stream of data" as a criterion for encryption parameter initialization (column 3, line 65 to column 4 line 13; Nardone '700).

To incorporate the variance of encryption key data as taught by Jones '730, the encryption granularity and density data as taught by Nardone '700, in addition to any other arbitrary encryption scheme, using the method taught by Leppek '501, would have been obvious to a person having ordinary skill in the art at the time of the invention as the combination of the same is necessary and explicitly taught therein as described above. Furthermore, it would have been obvious and necessary to a person having ordinary skill in the art at the time of the invention by the applicant to combine the to initialize the plurality of parameters as taught by Leppek '501, based on the sensitivity of the bitstream as taught by Nardone '700 as will be demonstrated below.

The motivation to vary encryption schemes on a bit stream and not just to use the Jones '730 encryption key variance method, is suggested by Leppek '501 teaching that "a fundamental characteristic of essentially all encryption operators or algorithms is

the fact that, given enough resources, almost any encryption algorithm can be broken. This, coupled with the fact that each encryption algorithm has a 'footprint', which is discernable in the scrambled data by a sophisticated data communications analyst, means that no data communication can be guaranteed as secure" (column 1, lines 54-60; Leppek '501). In other words, using the same encryption scheme on a continuous bit stream will eventually provide a statistically significant amount of data for a hacker to break the encryption scheme. Thus Leppek '501 discloses an invention that, "combines selected ones of plurality of different encryption operators" (column 1, lines 65-67; Leppek '501). Furthermore he goes on to teach, "The encryption routines ... need not be any particular type of encryption algorithm, and may be conventional encrypting operators, such as PGP, DES..." (column 4, lines 13-17; Leppek '501). Thus Leppek '501 teaches necessity for an implementer using the Jones '730 encryption key variance method, to vary the encryption scheme itself in order to reduce the cryptographic footprint of the bit stream.

The motivation to combine the "initializing a plurality of encryption parameters based on sensitivity of said stream of data" as taught by Leppek '501 into the Jones '730 / Nardone '700 / Leppek '501 combination is suggested by the fact that the Leppek '501 scheme delegates actual encryption to other algorithms and these algorithms inherently require initialization. Leppek '501 describes his disclosed invention as a "virtual encryption scheme" in which "the overall encryption operator itself does not actually perform any encrypting of the data. Instead, it assembles selected ones of a plurality of true encryption mechanisms into a cascaded sequence ..." (column 2, lines

6-13; Leppek '501). Thus the Leppek '501 invention would have to delegate to other encryption methods in order to actually encrypt the bit stream. Both the Jones '730 and Nardone '700, which are used in combination with Leppek '501 require initialization choices to be made (column 3; lines 26-40; Jones '730 and column 1, lines 50-59; Nardone '700). Thus in order to be used in combination with the invention of Leppek '501, the Jones '730 and Nardone '700 algorithms must be initialized. Furthermore, Nardone '700 teaches a motivation to set encryption granularity and density in order to reduce processing cycles (column 3, line 65 to column 4 line 13; Nardone '700). From this it is inherent that the initialization values should be set based on a tradeoff between processing overhead and adequate encryption. Thus it would have been obvious to a person having ordinary skill in the art at the time of the invention by the applicant to combine the to initialize the plurality of parameters as taught by Leppek '501, based on the sensitivity of the bitstream as taught by Nardone '700.

Furthermore, regarding Claim 9 as amended, Jones '730, Nardone '700, and Leppek '501 in combination address the issue of "multiple parameters" as described in paragraphs 9-10 below.

Regarding Claim 10, Jones '730 teaches all the limitations of Claim 1 as described above. Jones '730 does not explicitly teach the setting and varying of parameters, nor does it explicitly teach the use of MPEG compressed data as the data payload of a bit stream, nor does it explicitly teach the use of sensitivity of the bit stream for a criterion for setting parameters.

Leppek '501 teaches the use of multiple encryption algorithms as described above. Leppek '501 also teaches "setting a plurality of encryption parameters" (column 4, lines 52-66; Leppek '501) but does not use sensitivity of the bit stream as a criterion for initialization.

Nardone '700 teaches the varying of granularity and density encryption, specifically only encrypting a selected portion of a bit stream as described above. Nardone '700 also teaches "sensitivity of said stream of data" as a criterion for encryption parameter initialization (column 3, line 65 to column 4 line 13; Nardone '700). Moreover, Nardone '700 teaches an embodiment in which the bit stream is composed of MPEG compliant video data and MPEG compliant audio data including Dolby AC-3 data (column 2, lines 56-66; Nardone '700).

The motivation to vary encryption schemes on a bit stream and not just to use the Jones '730 encryption key variance method, is suggested by Leppek '501 teaching that "a fundamental characteristic of essentially all encryption operators or algorithms is the fact that, given enough resources, almost any encryption algorithm can be broken. This, coupled with the fact that each encryption algorithm has a 'footprint', which is discernable in the scrambled data by a sophisticated data communications analyst, means that no data communication can be guaranteed as secure" (column 1, lines 54-60; Leppek '501). In other words, using the same encryption scheme on a continuous bit stream will eventually provide a statistically significant amount of data for a hacker to break the encryption scheme. Thus Leppek '501 discloses an invention that, "combines selected ones of plurality of different encryption operators" (column 1, lines 65-67;

Leppek '501). Furthermore he goes on to teach, "The encryption routines ... need not be any particular type of encryption algorithm, and may be conventional encrypting operators, such as PGP, DES..." (column 4, lines 13-17; Leppek '501). Thus Leppek '501 teaches necessity for an implementer using the Jones '730 encryption key variance method, to vary the encryption scheme itself in order to reduce the cryptographic footprint of the bit stream.

The motivation to use MPEG compressed data as the payload of the Jones '730 / Nardone '700 / Leppek '501 in combination would be to make the combination applicable to the large MPEG market. A practitioner would have been motivated to use MPEG compliant data as the payload in the Jones '730 / Nardone '700 / Leppek '501 combination. In fact, the motivation to use the Nardone '700 granularity/density/delay encryption method was motivated by balancing processing overhead with encryption security in multimedia data.

The motivation to use sensitivity of stream data as a criterion for encryption parameter initialization in the Jones '730 / Nardone '700 / Leppek '501 combination is the same motivation as described in Claim 9.

Thus, it would have been necessary and obvious to a person having ordinary skill in the art to use MPEG compressed data and to use sensitivity of stream data as a criterion for encryption parameter initialization in the Jones '730 / Nardone '700 / Leppek '501 combination.

Furthermore, regarding Claim 10 as amended, Jones '730, Nardone '700, and Leppek '501 in combination address the issue of "multiple parameters" as described in paragraphs 9-10 below.

Regarding Claim 11, Jones '730 teaches the limitations of Claim 1 as described above. Jones '730 does not teach all the limitations of Claim 10. Furthermore, Jones '730 does not teach the setting of a, "plurality of encryption parameters ... establishing at least some of an encryption granularity, and initial encryption key, a density scale, a density, an encryption delay, and a key update data trigger for said stream of MPEG encoded data."

Leppek '501 teaches the use of multiple encryption algorithms as described above. Leppek '501 also teaches "setting a plurality of encryption parameters" (column 4, lines 52-66; Leppek '501) but does not use sensitivity of the bit stream as a criterion for initialization.

Nardone '700 teaches the varying of granularity and density encryption, specifically only encrypting a selected portion of a bit stream as described above. Nardone '700 also teaches "sensitivity of said stream of data" as a criterion for encryption parameter initialization (column 3, line 65 to column 4 line 13; Nardone '700). Moreover, Nardone '700 teaches an embodiment in which the bit stream is composed of MPEG compliant video data and MPEG compliant audio data including Dolby AC-3 data (column 2, lines 56-66; Nardone '700).

The motivation to combine Jones '730 / Nardone '700 / Leppek '501 in order to provide for the setting of "plurality of encryption parameters ... establishing at least

some of an encryption granularity, and initial encryption key, a density scale, a density, an encryption delay, and a key update data trigger," is described in the discussion regarding Claim 10 above.

The motivation to apply the Jones '730 / Nardone '700 / Leppek '501 combination method to a "stream of MPEG encoded data" by varying encryption schemes on a bit stream and not just to use the Jones '730 encryption key variance method, is suggested by Leppek '501 teaching that "a fundamental characteristic of essentially all encryption operators or algorithms is the fact that, given enough resources, almost any encryption algorithm can be broken. This, coupled with the fact that each encryption algorithm has a 'footprint', which is discernable in the scrambled data by a sophisticated data communications analyst, means that no data communication can be guaranteed as secure" (column 1, lines 54-60; Leppek '501). In other words, using the same encryption scheme on a continuous bit stream will eventually provide a statistically significant amount of data for a hacker to break the encryption scheme. Thus Leppek '501 discloses an invention that, "combines selected ones of plurality of different encryption operators" (column 1, lines 65-67; Leppek '501). Furthermore he goes on to teach, "The encryption routines ... need not be any particular type of encryption algorithm, and may be conventional encrypting operators, such as PGP, DES..." (column 4, lines 13-17; Leppek '501). Thus Leppek '501 teaches necessity for an implementer using the Jones '730 encryption key variance method, to vary the encryption scheme itself in order to reduce the cryptographic footprint of the bit stream.

As such it would have been necessary and obvious to a person having ordinary skill in the art apply the setting of the enumerated encryption parameters to MPEG encoded data.

Furthermore, regarding Claim 11 as amended, Jones '730, Nardone '700, and Leppek '501 in combination address the issue of "multiple parameters" as described in paragraphs 9-10 below.

Regarding Claim 22, Jones '730 teaches all the limitations of Claim 14 as described above. However, Jones '730 does not teach setting of multiple parameters based on sensitivity of the data.

Nardone '700 teaches the setting of a encryption granularity/density/delay and the selective encoding of a bit stream as described above. Nardone '700 also teaches "sensitivity of said stream of data" as a criterion for encryption parameter initialization as described above.

Leppek '501 teaches the rotating among several encryption algorithms as described above.

The motivation combine Jones '730, Nardone '700, and Leppek '501 in order to set of multiple parameters based on sensitivity of the data is described in the discussion above regarding Claim 9. As such, it would have been necessary and obvious for a person having ordinary skill in the art to modify Jones '730 to set multiple parameters based on sensitivity of data. Thus Claim 22 is rejected under 35 USC 103(a).

Regarding Claim 23, Jones '730 teaches all the limitations of Claim 14 as described above. Jones '730 does not explicitly teach the additional limitations of Claim

22 which Claim 23 incorporates. Furthermore, Jones '730 does not explicitly teach the use of a decompression decoder.

Nardone '700 teaches the setting of a encryption granularity/density/delay and the selective encoding of a bit stream as described above. Nardone '700 also teaches "sensitivity of said stream of data" as a criterion for encryption parameter initialization as described above. Furthermore, Nardone '700 explicitly teaches the use of compressed MPEG data (column 2, lines 56-66; Nardone '700), which implies an MPEG decoder, which in turn implies a decompression decoder.

Leppek '501 teaches the rotating among several encryption algorithms as described above.

The motivation to combine Jones '730 with Nardone '700 and Leppek '501, to set a plurality of encryption parameters is described in the discussion above regarding Claim 22.

The motivation to combine Jones '730 with Nardone '700 and Leppek '501 in order to carry compressed data and to use MPEG data is inherent in the the desire to carry MPEG data. In fact, Nardone '700 explicitly teaches the use of MPEG data. As a result, in order to render the data, adding an MPEG decoder after encryption is inherent in the Jones '730 / Nardone '700 / Leppek '501 combination. Since MPEG is inherently a compression standard, addition of the MPEG decoder constitutes adding a decompression decoder. As such, it would have also been necessary and obvious for a person having ordinary skill in the art to combine Jones '730 with Nardone '700 and Leppek '501 not only for the reasons enumerated in the discussion regarding Claim 22,

but also for the benefit of a decompression decoder. Thus Claim 23 is rejected under 35 USC 103(a).

Regarding Claim 24, Jones '730 teaches all the limitations of Claim 14 above. However, Jones '730 does not explicitly teach all the limitations of Claim 23 which Claim 24 incorporates. Furthermore, Jones '730 does not explicitly teach the use of MPEG, video and audio, and Dolby AC-3 data for the data payload.

Nardone '700 teaches the setting of a encryption granularity/density/delay and the selective encoding of a bit stream as described above. Nardone '700 also teaches "sensitivity of said stream of data" as a criterion for encryption parameter initialization as described above. Furthermore, Nardone '700 explicitly teaches the use of compressed MPEG data (column 2, lines 56-66; Nardone '700), which implies an MPEG decoder.

Leppek '501 teaches the rotating among several encryption algorithms as described above.

The motivation to combine Jones '730 / Nardone '700 / Leppek '501 to set a plurality of encryption parameters and to use compressed data is described in the discussion regarding Claim 23 above.

The motivation to combine Jones '730 / Nardone '700 / Leppek '501 to use MPEG data is inherent in the discussion regarding Claim 23 above. The counterexample in the discussion above on Claim 23 explicitly refers to the Nardone '700 in which MPEG, video and audio, and Dolby AC-3 data is used for the data payload (column 2, lines 56-66; Nardone '700). Thus it would have been obvious for a person having ordinary skill in the art to combine Jones '730 / Nardone '700 / Leppek

'501 in order to set multiple encryption parameters, and to use MPEG/AC-3 multimedia data for a data payload. Thus Claim 24 is rejected under 35 USC 103(a).

Regarding Claim 25, Jones '730 teaches all the limitation of Claim 14 above. However, Jones '730 does not explicitly teach all the limitations of Claim 23 which Claim 25 incorporates. Furthermore, Jones '730 does not explicitly teach the limitation of initializing a number of encryption parameters.

Nardone '700 teaches the setting of a encryption granularity/density/delay and the selective encoding of a bit stream as described above. Nardone '700 also teaches "sensitivity of said stream of data" as a criterion for encryption parameter initialization as described above. Furthermore, Nardone '700 explicitly teaches the use of compressed MPEG data (column 2, lines 56-66; Nardone '700), which implies an MPEG decoder.

Leppek '501 teaches the rotating among several encryption algorithms as described above. Leppek '501 also teaches the initialization of encryption parameters as described above.

The motivation to combine Jones '730 / Nardone '700 / Leppek '501 in order to meet the limitations of Claim 23 is described in the above discussion regarding Claim 23.

The motivation to combine Jones '730 / Nardone '700 / Leppek '501 in order to meet initialize multiple encryption parameters is described in the above discussion regarding Claim 11.

Thus it would have been obvious for a person having ordinary skill in the art to combine Jones '730 / Nardone '700 / Leppek '501 to meet the limitations of Claim 25. Thus Claim 25 is rejected under 35 USC 103(a).

5. Claims 4 and 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Jones '730 in view of Nardone '700 and Leppek '501 and in further view of "Digital Television Achieves Maturity" by Leonardo Chiariglione, copyrighted 1998 (Chiariglione '98).

Claim 4:

Regarding Claim 4, Jones '730 / Nardone '700 / Leppek '501 in combination teach all the limitations of Claim 3 as described above. Furthermore, Nardone '700 teaches varying encryption schemes via a policy (column 2, lines 40-46; Nardone '700) and furthermore in a disclosed embodiment teaches varying the policy dynamically (column 4, lines 23-42; Nardone '700). However, Jones '730 / Nardone '700 / Leppek '501 do not teach multiplexing in the variance information into the encrypted bit stream.

Chiariglione '98 teaches multiplexing in the variance information into the encrypted bit stream (page 2, line 32 to page 3, line 8, and Figure 1; Chiariglione '98).

To incorporate the multiplexing in of variance information into the encrypted bit stream as taught by Chiariglione '98, to the Jones '730 / Nardone '700 / Leppek '501 combination, would have been obvious to a person having ordinary skill in the art at the time of the invention as the combination of the same is necessary and explicitly taught therein as will be demonstrated below.

The motivation to transmit dynamically varying encryption policy information via the Chiariglione '98 within the context of the Jones '730 / Nardone '700 / Leppek '501 combination is suggested by the fact that both disclosures are refer to the encryption/decryption of multimedia data. Selectively encrypt a bit stream as taught by Nardone '700 is a direct consequence of handling multimedia data. The Chiariglione '98 teaching discusses the MPEG-2 specification, which discloses use of EMM and ECM messages multiplexed into the bit stream in order to provide access control information dynamically. In order to take advantage of the MPEG market, the inventor would have been motivated to use of EMM and ECM messages multiplexed into the bit stream as taught by the MPEG specification. As such, it would have been necessary and obvious to apply the Chiariglione '98 teaching with the Jones '730 / Nardone '700 / Leppek '501 combination in order to be compliant with the MPEG specification and thus be salable in the MPEG market. Thus Claim 4 is rejected under 35 USC 103(a).

Claim 21:

Regarding Claim 21, Jones '730 teaches all the limitations of Claim 14. However, Jones '730 does not teach multiplexing in the encryption parameter in with the bit stream.

However, the Jones '730 / Nardone '700 / Leppek '501 / Chiariglione '98 combination described in the discussion regarding Claim 4 above teaches multiplexing in the encryption parameter in with the bit stream.

It would have been necessary and obvious for a person having ordinary skill in the art to modify Jones '730 to multiplex in the encryption parameter in with the bit

stream as described in the discussion above regarding Claim 4. Thus Claim 21 is rejected under 35 USC 103(a).

6. Claims 28, 29, 32, and 34-38 are rejected under 35 U.S.C. 103(a) as being unpatentable in view of Jones '730 in view of Warren '937, and in further view of Nardone '700 and moreover in view of Leppek '501.

<u>Claims 29 and 32-25 (as amended):</u>

Regarding Claims 28, 29, 32, 34, and 35, Jones '730 teaches corresponding limitations in all the aforementioned claims with the exception of explicitly teaching a program storage device. Refer to the discussions regarding Claims 2, and 5-8 respectively.

Warren '937 teaches a program storage device (column 6, lines 28-36; Warren '937) in an encrypting system.

The motivation to apply the encryption scheme of Jones '730 to the program storage device of Warren '937 is suggested by Warren '937, "it would be desirable to provide an electronic copy management scheme for controlling the reproduction of proprietary data" (column 1, lines 36-38; Warren '937). In fact, Warren '937 discloses one such invention. Furthermore, the motivation to use the method of Jones '730 is suggested by Jones '730, "For increased data security, the encryption key value may be changed frequently to further reduce the likelihood that an unauthorized party may decipher the data" (column 1, lines 22-25; Jones '730). Thus an implementer who used the program storage device and copy management method of Warren '937, who

desired to reduce the ability to hack the data would be motivated to add the encryption method of Jones '730.

Furthermore, Jones '730 does not explicitly teach the additional limitations regarding dynamically varying multiple encryption parameters employed for each portion of a stream of data.

Nardone '700 teaches dynamically changing encryption parameters as described in paragraphs 9-10 below. However, Nardone '700 does not explicitly teach setting multiple parameters.

Leppek '501 teaches setting multiple parameters as described in paragraphs 9-10 below.

It would have been obvious to a person having ordinary skill in the art to combine Nardone 700 and Leppek '501 with Jones '730 and Warren '937 on the same basis as described in paragraphs 9-10 below.

Claims 36-38:

Regarding Claims 36-38, Jones '730, Nardone '700, and Leppek '501 in combination teach corresponding limitations in all the aforementioned claims with the exception of explicitly teaching a program storage device. Refer to the discussions regarding Claims 3, 14, 10, and 11 respectively.

The motivation to apply the encryption scheme of the Jones '730 / Nardone '700 / Leppek '501 combination to the program storage device of Warren '937 is suggested by Warren '937, "it would be desirable to provide an electronic copy management scheme for controlling the reproduction of proprietary data" (column 1, lines 36-38; Warren '937).

In fact, Warren '937 discloses one such invention. Furthermore, the motivation to use the method of the Jones '730 / Nardone '700 / Leppek '501 combination is suggested by Warren '937, "it is assumed that the source material which is stored on the media is compressed data, and that the media is a laser disk, compact disk, or DVD" (column 6, lines 28-31; Warren '937). The context of the Warren '937 invention is that of multimedia data. As discussed above, the Jones '730 / Nardone '700 / Leppek '501 provides a cryptographic combination motivated to be applied to multimedia data. Thus a practitioner ordinarily skilled in the art would be motivated to apply the Jones '730 / Nardone '700 / Leppek '501 method to the program storage device of Warren '937. Thus Claims 30, and 36-38 are rejected under 35 USC 103(a).

Furthermore, regarding Claims 36-38 as amended note that Nardone '700 teaches dynamically changing encryption parameters and Leppek '501 teaches setting multiple parameters as described in paragraphs 9-10 below.

7. Claim 31 is rejected under 35 U.S.C. 103(a) as being unpatentable over Jones '730, Nardone '700, Leppek '501, and Chiariglione '98 in view of Warren '937.

<u>Claim 31:</u>

Regarding Claim 31, Jones '730, Nardone '700, Leppek '501, and Chiariglione'98 teach corresponding limitations with the exception of explicitly teaching a program storage device as described in the discussion regarding Claim 4 above.

Warren '937 teaches a program storage device (column 6, lines 28-36; Warren '937) as described in the discussion regarding Claim 28 above.

The motivation to apply the encryption scheme of the Jones '730 / Nardone '700 / Leppek '501 / Chiariglione '98 combination to the program storage device of Warren '937 is suggested by Warren '937, "it would be desirable to provide an electronic copy management scheme for controlling the reproduction of proprietary data" (column 1, lines 36-38; Warren '937). In fact, Warren '937 discloses one such invention. Furthermore, the motivation to use the method of the Jones '730 / Nardone '700 / Leppek '501 / Chiariglione '98 combination is suggested by Warren '937, "it is assumed that the source material which is stored on the media is compressed data, and that the media is a laser disk, compact disk, or DVD" (column 6, lines 28-31; Warren '937). The context of the Warren '937 invention is that of multimedia data. As discussed above, the Jones '730 / Nardone '700 / Leppek '501 / Chiariglione '98 provides a cryptographic combination, including multiplexing encryption data. Thus a practitioner with ordinary skill in the art would be motivated to apply the Jones '730 / Nardone '700 / Leppek '501 / Chiariglione '98 method to the program storage device of Warren '937.

Response to Arguments

8. Applicant's arguments filed 15 August 2005 have been fully considered but they are not persuasive.

9. Examiner notes the set of limitations under contention as follows:

- "dynamically changing simultaneously multiple encryption parameters used to encrypt the stream of data as the stream of data is passing through the encryption unit" [Amendment: p. 13, lns. 18-20]; and
- "signaling the dynamic change in the encryption parameters from the encryption unit to the decryption unit" [Amendment: p. 14, lns. 21-22].

10. Examiner now addresses these specific limitations over U.S. Patent No. 5,412,730 issued to Jones (hereafter Jones '730), U.S. Patent No. 5,805,700 issued to Nardone et al. (hereafter Nardone '700), and U.S. Patent No. 5,933,501 issued to Leppek (hereafter Leppek '501).

Regarding "dynamically changing simultaneously multiple encryption parameters used to encrypt the stream of data as the stream of data is passing through the encryption unit":

- Encryption devices send encrypted data to decryption devices. It is well known in the art to vary the means of encryption in an encryption device in order to improve security. Jones '730 teaches one such invention wherein an encryption device whose means of encryption involves an encryption key and whose means of varying encryption is by varying the encryption key [Jones '730: col. 1, lns. 22-35]. While varying the encryption key is one was to vary the means of encryption, it is not the only way to vary the means of

encryption. The insight of Jones '730 is in the varying of the means of encryption.

- Dynamically changing encryption parameters used to encrypt the stream of data is a valid way to vary the means of encryption. Nardone '700 teaches specifying encryption parameters via a policy (i.e. the degree of selective encryption in order to degrade video image) [Nardone '700: col. 1, lns. 40-50]. Furthermore, Nardone '700 teaches the dynamic changing of encryption policies [Nardone '700: col. 1, lns. 51-59]. Since a policy teaches the setting of encryption parameters and dynamic changing of encryption policies reads on dynamic changing of encryption parameters. While varying the degree of selective encryption in order to degrade video image is one possible encryption parameter to vary, it is not the only encryption parameter to vary. The insight of Nardone '700 is the use of policies that specify parameters to vary and the dynamic changing simultaneously multiple encryption parameters via dynamically changing policies.
- Where Nardone '700 is not explicit about setting multiple parameters in a policy, Leppek '501 is explicit about setting multiple encryption parameters. Leppek '501 teaches applying multiple encryption operators [Leppek '501: col. 1, ln. 64 to col. 2, ln. 5]. Encapsulating the setting of multiple encryption parameters of Leppek '501 into a single policy of Nardone '700, and having a multiplicity of different policies (i.e. different multiple encryption parameters set), and dynamically changing policies as taught by Nardone '700 [supra],

fully reads on dynamically changing simultaneous multiple encryption parameters. The insight of Leppek '501 is the application of multiple encryption operators at once.

- The motivation to combine Nardone '700 with Jones '730 is suggested by Nardone '700, i.e. the policies of Nardone '700 teach partial encryption in order to save processing cycles on encrypting data. Applying the policies of Nardone '700 to Jones '730 creates a combination in which enables selective encryption of the bit stream to save cycles and provide fast encryption of streaming data [Nardone '700: col. 1, lns. 45-50]. The insight of this combination is rather than Jones '730 simply changing encryption keys, Jones '730 can change policies as per Nardone '700 where each policy contains an independent setting of encryption parameters.
- The motivation to apply the multiple parameters of Leppek '501 with the Nardone '700 and Jones '730 combination, i.e. to have each of a plurality of policies of Nardone '700 specify multiple parameters, and further to have said plurality of policies be dynamically changed, is suggested by Leppek '501 which states that varying encryption schemes reduces cryptographic footprint and thus increases security [Leppek '501: col. 1, lns. 54-60; col. 1, lns. 65-67]. This is analogous to the teaching of Jones '730 which states that changing an encryption parameter increases data security [Jones '730: col. 1, lns. 15-21]. The insight of applying Leppek '501 to the Nardone '700 and Jones '730 combination is that Jones '730 can change policies as per

Nardone '700 where each policy contains an independent setting of a multiplicity of encryption parameters.

Regarding "signaling the dynamic change in the encryption parameters from the encryption unit to the decryption unit":

- The Jones '730 patent, still requires the exchange of random number seed values and interval values between the encryptor and decryptor [Jones '730: col. 1, ln. 66 to col. 2, ln. 7]. The exchange of random number seed values and/or interval values constitutes and event that causes a change in encryption by encryptor and decryptor.
- Within the context of the Jones '730, Nardone '700, and Leppek '501 combination,
- On this basis, the Jones '730, Nardone '700, and Leppek '501 combination reads on "signaling the dynamic change in the encryption parameters from the encryption unit to the decryption unit."

It is noted that all of Applicant's arguments filed 15 August 2005 against the rejections under 35 U.S.C. 103 have been previously made either in the Request for Reconsideration filed 17 May 2004 or the Appeal Brief filed 25 August 2004, and that no new limitations since have been added to the claims that would affect the validity of these arguments. These arguments were fully answered in the Advisory Action mailed 26 August 2004 and the Examiner's Answer mailed 14 December 2004, respectively,

and the Examiner's specific counterarguments as they apply to the claims as presently written were in no way refuted in the BPAI's reversal. Applicant's arguments filed 15 August 2005 are therefore not being further addressed here.

Conclusion

11. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

12. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

U.S. Patent No. 6,157,719 to Wasilewski et al. teaches to the varying of encryption keys in a subscription television system.

13. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Matthew E. Heneghan, whose telephone number is (571) 272-3834. The examiner can normally be reached on Monday-Friday from 8:30 AM - 4:30 PM Eastern Time.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse, can be reached at (571) 272-3838.

Any response to this action should be mailed to:
Commissioner of Patents and Trademarks
P.O. Box 1450
Alexandria, VA 22313-1450
Or faxed to:
(571) 273-3800

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (571) 272-2100.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should

you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

MEH MEH

December 14, 2005

David Y. Jung
Primary Examiner
12/23/06